



REBOOT:

RE-EXAMINING THE
STRATEGIES NEEDED
TO SUCCESSFULLY
ADOPT HEALTH IT

By Senators Thune, Alexander, Roberts, Burr, Coburn, Enzi

oApril 16, 2013

EXECUTIVE SUMMARY

The advancement of health information technology holds the promise of increasing efficiency in the health care system; reducing costs for payers, providers, and patients; and improving quality of care for patients and their families. To achieve these goals, in 2009 Congress passed legislation devoting some \$35 billion to promote providers' adoption and use of federally certified health information technology (health IT).¹ This law, the Health Information Technology and Economic and Clinical Health (HITECH) Act, was included as part of President Obama's economic stimulus, the American Recovery and Reinvestment Act of 2009 (ARRA).

However, while promoting the use of health IT is a laudable goal, a growing body of objective analysis and empirical data suggests the program needs to be recalibrated to be effective. Congress and the administration need to work together to "reboot" the program to accomplish the aims of meaningful use and interoperability and ensure appropriate stewardship of taxpayer dollars in the process.

The key implementation deficiencies can be summed up in five points:

- **Lack of Clear Path Toward Interoperability.** The HITECH Act, a \$35 billion program of grants and incentive payments in ARRA, was created to promote the use of electronic health records (EHRs) among hospitals and physicians, with the ultimate goal of incentivizing the adoption and use of health information technologies meeting a certain data standard so that providers can share patient health data nationwide.² The ability to share data, it was said, would reduce the overall need for as many tests, arm providers with better patient information, and enhance the quality of patient care. However, to achieve this aim, having interoperable systems is necessary. Unfortunately, early reports suggest that federal incentive payments are being made without clear evidence that providers can achieve "meaningful use," or the ability to use the health IT program internally, and without an adequate plan to ensure providers can share information with each other.

RESPONSE:

The underlying issue is not technology. Technology currently exists to fulfill the HITECH interoperability requirements. There is a highly competitive environment within the healthcare community, created by the meaningful use program, which includes hundreds of certified EHR vendors. Those vendors, especially the top ten that control over 70% of the medical practice and hospital market, do not want to cooperate with their competitors. Professionals with academic and medical backgrounds who serve on various advisory committees are pursuing regulatory solutions, whereas in reality, these regulatory changes are only exacerbating the existing interoperability issues. Physicians and their staff understand the need to communicate. Unfortunately, communication modes in the healthcare community are significantly outdated. Internet-based efficiencies will improve health care from many angles through better communications. However, cooperation on the part of vendors is critical to advance these technologies.

In a recent meeting between a top EHR ambulatory vendor and a top Hospital Information System (HIS) vendor, the two entities attempted to achieve system-wide interoperability mandating the use of one of their systems. This vendor-based approach is not effective, considering the hundreds of available, usable certified systems. A more effective approach would be to establish standard

criteria to capture health information data such as Continuity of Care Documents (CCD) / Continuity of Care Records (CCR), and thereby forcing vendors to capture and identify discrete patient data as an initial step. In fact, this type of approach, at least partially, is in place today.

- **Increased Costs.** Members of Congress and policy analysts across the political spectrum have promoted health IT as one tool to help bring down health care costs. Through efficiencies in storing and sharing records and ordering and coordinating patient care, as well as structural savings through better data and research, cost savings are estimated in the billions of dollars in the next decade alone. For example, the Congressional Budget Office estimated that the HITECH Act will save the Medicare and Medicaid programs a total of about \$12.5 billion through 2019.³ However, early reports raise concerns that health IT may have actually accelerated the ordering of unnecessary care as well as increased billing for the same procedures.
- **Lack of Oversight.** Based on Department of Health and Human Service's Inspector General and Government Accountability Office (GAO) reports as well as stakeholder comments and a review of program data, it is increasingly clear that the Administration does not have adequate mechanisms in place to prevent waste and fraud in its health IT programs. Too often we have heard stories of "money spent" being used as a metric of success, rather than specific, concrete program goals and tangible deliverables that are focused on achieving interoperability. There have been reports of taxpayer dollars being paid to providers who cannot or do not have to demonstrate that the technology is actually used as prescribed, because the administration relies on provider "self-attestation" in many cases to determine eligibility for payments. In some cases, contractors receiving government funds may be creating obstacles to interoperability. In other cases, providers who have previously received federal incentive grants are reportedly now forced to adopt less advanced technologies to meet current standards, effectively forcing them to scrap prior federally subsidized investments.

¹ \$35 billion includes \$32.7 billion in incentive payments and nearly \$2 billion in grants. Redhead, Stephen C. "*The Health Information Technology and Economic and Clinical Health (HITECH Act)*." Congressional Research Service, Report No. R40101. 2009.

² "HITECH Act." [HealthIT.gov](http://www.healthit.gov/policy-researchers-implementers/hitech-act-0), <http://www.healthit.gov/policy-researchers-implementers/hitech-act-0>

³ Redhead, Stephen C. "*The Health Information Technology and Economic and Clinical Health (HITECH Act)*." Congressional Research Service, Report No. R40101. 2009

RESPONSE:

There is willingness on the part of the providers to comply with and adopt an EHR system with the hope that the conversion to electronic health records will save time, money, create efficiencies, and help deliver better healthcare through modern communications. HITEC projects, whether inside with primary providers or outside with specialists and dentists, are working to ensure that the systems are being used from year to year as intended, and that the requirements for incentive funding are addressed. In almost every instance, audits are performed by state and/or federal Medicaid and Medicare program officials. The HITEC projects throughout the country could and should fulfill their obligation to their provider members by requiring field agents to take an active role in maintaining a high quality of EHR usage at the provider level that can stand up to an audit. In order to accomplish this, the compensation to field agents in relation to administrative personnel administering the program at the HITEC level needs to be re-evaluated. Instead of spending money on HITEC administrative infrastructure, the focus of service needs to be redirected to the field support, as these officials provide leadership and advice to the provider/medical practice. These people can be direct employees, well-compensated independent agents that have the direct relationship with providers, and their staff will produce far higher quality encounters.

- **Patient Privacy at Risk.** We are concerned the administration has not done enough to protect sensitive patient information in a cost-effective manner. Among other problems, regulations related to payments made to providers do not require providers to demonstrate that the technology is secure; consequently, patients' sensitive, personal medical information may be at risk. In fact, the Inspector General of the U.S. Department of Health and Human Services found that the security policies and procedures at the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology – two federal entities which oversee the administration of the health IT program – are lax and may jeopardize sensitive patient data.⁴ Being proactive in addressing privacy and security concerns while minimizing the additional burden on providers is a critical part of ensuring the long-term success of EHRs. Further, problems with data entry, computer programming errors, and other unforeseen complications can affect the security of patient data and have the potential to jeopardize patient care.
- **Program Sustainability.** For providers who have accepted grants or incentive payments, it is unclear how much it will cost to maintain their health IT systems after the initial grant money and incentive payments run out. For example, in 2015, incentive payments in most scenarios cease, and providers face penalties in the way of reduced Medicare reimbursements if they do not comply with federal requirements. Even worse, these penalties are most likely to affect small providers who may not have the economies of scale needed to make complex electronic systems cost-effective. Moreover, the complicated patchwork of overlapping reporting and compliance requirements is already placing ongoing compliance burdens on all participating providers. We are concerned that compliance and maintenance costs for providers may be unreasonably burdensome.

RESPONSE:

Positioned properly so that no federal or state laws are in violation, there is an opportunity to provide sustainability beyond the end of the federal incentive program. The current incentive program should only “prime the pump.” Possibilities exist to revenue share with the providers and the HITEC projects themselves in many areas and transition them from dependency to independence. For example, through a national healthcare communications network, direct

access to providers and their staff in a non-invasive, non-intrusive manner is very possible and will be very valuable. Providers have repeatedly affirmed that encounters with pharmaceutical, medical device, and supply representatives are very important. However, these encounters should not take place when a provider is administering health care to patients. A national communications network would effectively allow the provider to control the time and place of exchanges with representatives, allowing the provider to balance these encounters with patient needs. In addition, there is extreme value in de-identified patient statistics, underwriting or support of the EHR cost from insurance companies, labs, imaging center, etc.

This white paper addresses each area of concern in depth. We present this paper as part of our broader effort to solicit feedback from the administration and foster an ongoing conversation with the stakeholder community – health care providers, technology vendors, and others. It is our goal to work cooperatively with the administration, our colleagues in both parties in Congress, and the American people to learn more about the issues raised here and to address the problems identified.

⁴ Lewis, Nichole. “Federal Agencies Fail Health IT Security Audits.” *Information Week*. May 18, 2011.
<http://www.informationweek.com/healthcare/security-privacy/federal-agencies-fail-health-it-security/229502471>

Table of Contents

Introduction	4
Background	6
I. Lack of Clear Path Toward Interoperability	10
II. Misuse of EHRs May Actually Increase Health Care Costs	15
III.	I
nsufficient Oversight Has Put Taxpayer Money at Risk.....	18
IV.	L
ong-Term Questions on Data Security and Patient Safety Remain	21
V. Questions Remain About Long-Term Sustainability of the EHR Program	23
Conclusion	27

Introduction

Since the dawn of the modern communications revolution, transformations in health information technology (health IT) have been evolving at an increasingly rapid pace. Today's creative and powerful health IT solutions have the potential to dramatically upend the status quo and reshape the delivery of health care in our country. Today more than ever, Americans are searching for medical information online, checking drug interactions or symptoms with their smart phones, or e-mailing their family doctors. Physicians can access digital records of a patient even if they are in another city, state, or country. Clinical notes are recorded with increasing speed and ease, and other transformations offer the promise of increased efficiency, reduced costs, and improved quality of care. However, the details of federal law and regulation may be inadvertently incentivizing unworkable, incoherent policy goals that ultimately make it difficult to achieve interoperability.

In 2009, the Health Information Technology and Economic and Clinical Health (HITECH) Act was passed as part of the American Recovery and Reinvestment Act (ARRA).⁵ The HITECH Act was enacted on the heels of several existing federal incentive programs designed to promote the adoption and effective use of electronic health records (EHRs). The ultimate goal of this act was to create standards for the secure exchange of patient data nationwide, whether the site of care was a hospital or a local primary care physician's office. In other words, the goal of the HITECH Act was for providers across the country to be able to adopt technology that would allow them to store and access EHRs, to share them seamlessly in a timely manner, and to create a network for providers' systems to be interoperable. ARRA appropriated approximately \$35 billion for the Office of National Coordinator for Health IT and the Centers for Medicare and Medicaid Services (CMS) to achieve this goal. Now, nearly four years after the enactment of the HITECH Act, and after hundreds of pages of regulations implementing the program, we see evidence that the program is at risk of not achieving its goals and that \$35 billion in taxpayer money is being spent ineffectively in the process.



This paper addresses the following five concerns:

- **Lack of Clear Path Toward Interoperability**
- **Increased Costs**
- **Lack of Oversight**
- **Patient Privacy at Risk**
- **Program Sustainability**

⁵ American Recovery and Reinvestment Act of 2009, Public Law 111-5. <http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf>

Of the \$35 billion in incentive payments and grants authorized by ARRA, as of February 28, 2013, CMS estimated it has paid out nearly \$12.7 billion in incentive payments.⁶ Of that sum, nearly \$1.2 billion was paid in December of 2012 alone.⁷ With so many dollars flowing out of CMS, Congress has the fiduciary responsibility to ensure that these taxpayer dollars are being used to efficiently accomplish the end goal of reduced health care costs through the appropriate sharing and use of health information.

We present this white paper in an effort to initiate a dialogue with the administration and the stakeholder community. The purpose of this paper is to foster cooperation between all stakeholders – including providers, patients, EHR vendor companies, and the Department of Health and Human Services – to address the issues raised in this paper, evaluate the return on investment to date, and ensure this program is implemented wisely.

⁶ Centers for Medicare and Medicaid Services. *EHR Incentive Program Report, February 2013*.

http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Feb_EHRIncentiveProgramsPaymentsReg_SummaryReport.pdf

⁷ Conn, Joseph. “Whopping \$1.2 billion in EHR Payments in December.” *Modern Healthcare*. January 8, 2013.

<http://www.modernhealthcare.com/article/20130108/NEWS/301089956>

Background

The Health Information Technology for Economic and Clinical Health (HITECH) Act is the most recent major health IT law, but it followed on the heels of the establishment of a patchwork of programs and laws first created in 1996. These laws all attempt to promote the widespread adoption of health IT while ensuring patient privacy is protected. “Health information technology,” as referred to in federal law and in this white paper, broadly refers to electronic storage of records, electronic billing, electronic ordering of tests and procedures, and even a shared, interoperable network to allow providers to communicate with each other. Health IT initiatives undertaken by the private sector, such as mobile applications used by insurance plans, are not addressed in this white paper.

Underlying much of the federal government’s health IT policy efforts has been an assumption that health IT will help to improve outcomes for patients and reduce costs in the health care system.⁸ The expectation has been that providers will be able to coordinate and provide care more efficiently with comprehensive records stored at their fingertips. The fast and easy sharing of patient data across providers should improve patient outcomes, the conventional wisdom goes, by, for example, identifying harmful drug interactions, reducing unnecessary duplicate testing, and helping physicians manage patients with multiple conditions.

Landscape of Health IT Policy

Multiple overlapping programs form the framework of federal health IT policy. The main laws and programs are outlined as follows:

HITECH Act. The HITECH Act of 2009, adopted as part of the American Recovery and Reinvestment Act of 2009 (ARRA), promotes widespread health IT adoption.⁹ The act codified the Office of the National Coordinator for Health Information Technology, which is tasked with establishing standards necessary to share health care data nationally through a secure digital environment. It also established a number of financial incentives, including grant programs and Medicare and Medicaid incentive payments, to promote adoption of health IT among health care practitioners. (See summary below of HITECH Act’s major provisions.)

HIPAA. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 created federal requirements for the protection of personal health information.¹⁰ These include provisions regarding security standards to safeguard electronic health information against unauthorized access, use, and disclosure, such as off-site backups, restricting access to computers, passwords, and encryption, and rules about when and how protected health information can be disclosed. The HITECH Act of 2009 made modifications to HIPAA to expand enforcement provisions, and the final rule implementing these additional federal mandates was published in the Federal Register on

⁸ Giroi, Federico, et al. *Extrapolating Evidence of Health Information Technology Savings and Costs*. RAND Health. 2005. http://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG410.pdf

⁹ American Recovery and Reinvestment Act of 2009. Public Law 111-5. <http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf>

¹⁰ The Health Insurance Portability and Accountability Act of 1996. Public Law 104-191. <http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>

January 25, 2013.¹¹ Failure to comply with HIPAA results in civil penalties of up to \$50,000 per violation and \$1,500,000 per year.¹²

PQRS. The Physician Quality Reporting System (PQRS) was initially created by the Tax Relief and Health Care Act of 2006.¹³ What was originally a voluntary program that created an electronic reporting system under Medicare for providers to report clinical quality measures now has its own set of penalties of reduced Medicare reimbursements for non-participating providers.¹⁴

eRx Incentive Program. The Electronic Prescribing (eRx) Incentive Program was created by the Medicare Improvements for Patients and Providers Act of 2008, and provides incentive payments to eligible physicians who e-prescribe Medicare Part D medications using a qualified system.¹⁵ Starting last year, providers who did not use eRx were subject to reduced Medicare reimbursements as a penalty.

Grant Programs. ARRA appropriated \$2 billion in the HITECH Act for grants to fund health IT infrastructure and grants to states for low-interest health IT loans. The Agency for Healthcare Research and Quality (AHRQ) has awarded \$300 million in federal grant money to over 200 projects in 48 states to promote access to and encourage adoption of health IT.¹⁶ Over \$150 million in Medicaid Transformation Grants have been awarded to 35 states and territories for health IT initiatives in the Medicaid program, pursuant to the Deficit Reduction Act of 2005.¹⁷



¹¹ Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Final Rule, 78 Fed. Reg. 5566, January 25, 2013.

<http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf>

¹² Penalties for HIPAA violations are found at 42 USC § 1320d-5.

<http://www.gpo.gov/fdsys/pkg/USCODE-2011-title42/pdf/USCODE-2011-title42-chap7-subchapXI-partC-sec1320d-5.pdf>

¹³ Tax Relief and Health Care Act of 2006, Public Law 109-432.

<http://www.gpo.gov/fdsys/pkg/PLAW-109publ432/pdf/PLAW-109publ432.pdf>

¹⁴ “Electronic Prescribing (eRx) Incentive Program.” Centers for Medicare and Medicaid Services. Last modified September 19, 2012. <http://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/ERxIncentive/index.html?redirect=/erxincentive>

¹⁵ Medicare Improvements for Patients and Providers Act of 2008. Public Law 110-275.

<http://www.gpo.gov/fdsys/pkg/PLAW-110publ275/pdf/PLAW-110publ275.pdf>

¹⁶ “Health IT at AHRQ.” Agency for Healthcare Research and Quality. Last modified November 2011.

<http://healthit.ahrq.gov/portal/server.pt/community/about/562>

¹⁷ Hayes, Heather. “CMS Awards More Medicaid Transformation Grants.” Government Health IT. October 5, 2007.

<http://www.govhealthit.com/news/cms-awards-more-medicare-transformation-grants>

Federal Offices, Initiatives. A number of entities were created by Congress and the administration to address health IT implementation issues. The Office of National Coordinator for Health IT (ONC) established the Health Information Security and Privacy Collaboration (HISPC) to develop a national privacy and security framework. The Healthcare Information Technology Standards Panel (HITSP), another ONC creation, is a public-private effort to develop standards for the certification of health IT products. The Department of Health and Human Services secretary created the National eHealth Collaborative (NeHC), a public-private advisory body to make recommendations on health IT adoption and usability. The AHRQ created the online National Resource Center for Health IT to serve as a public resource for information on health IT. Finally, the Health Resources and Services Administration (HRSA) works to improve access and use of health IT for safety net providers.

HITECH ACT

While the HITECH Act built on previous federal efforts to encourage health IT adoption, it is now the primary piece of legislation directing the bulk of federal health IT policies and programs.¹⁸ In addition to \$2 billion in grants funded through the HITECH Act, the Congressional Budget Office (CBO) estimates that \$32.7 billion will be spent from 2009-2019 in Medicare and Medicaid through HITECH. Notably, according to CBO estimates at the time the law was enacted, HITECH was *not* required for the adoption and use of health IT to spread. In fact, without HITECH, the CBO predicted 45 percent of hospitals and 65 percent of physicians would have adopted Health IT by 2019. With HITECH, CBO estimated 70 percent of hospitals and 90 percent of physicians will adopt health IT in that time frame.¹⁹ This white paper will examine the accuracy of that estimate at a later point. HITECH includes four major provisions.

First, HITECH codified the Office of National Coordinator for Health IT, which has as its goal the establishment of standards that support the nationwide electronic exchange of health information (called

“interoperability”) in a secure computer network. Hence, the Office of National Coordinator for Health IT is building the National Health Information Network (NHIN), a nationwide, secure platform that connects health networks using shared standards and policies (a “network of networks”). The Office of the National Coordinator for Health IT also established HISPC to develop a national privacy and security framework and HITSP to develop standards for the certification of health IT products.



Second, HITECH established \$2 billion in grant programs to fund investment in health IT infrastructure, resource centers, workforce programs, standards development, research projects, and privacy and security programs, as well as grants to

¹⁸ This does not include DOD and VA efforts.

¹⁹ Redhead, Stephen C. “*The Health Information Technology and Economic and Clinical Health (HITECH Act)*.” Congressional Research Service, Report No. R40101. 2009.

states to provide low-interest loans to help providers finance health IT. As of March 1, 2013, \$1.985 billion of that \$2 billion has been allocated.

Third, HITECH funds Medicare incentive payments to encourage doctors and hospitals to adopt and use certified electronic health records (EHRs). The incentive payments will be phased out over time and replaced with penalties for not “meaningfully using” health IT. Additionally, HITECH authorized the federal government to pay 100 percent of the cost to adopt certified EHR systems for certain Medicaid providers. To date, a total of \$12.7 billion has been distributed to 388,593 providers or hospitals.²⁰

Fourth, HITECH amended HIPAA to expand and strengthen certain privacy and security requirements. HITECH created a right to be notified in the event of a breach of identifiable health information. It also increases civil penalties for certain HIPAA privacy violations.

While CBO estimated that HITECH would save the Medicare and Medicaid programs a total of \$12.5 billion during the budget window, the net cost of HITECH over the ten-year scoring period was \$20.8 billion.²¹

²⁰ Centers for Medicare and Medicaid Services. *EHR Incentive Program Report*, February 2013.

http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Feb_EHRIncentiveProgramsPaymentsReg_SummaryReport.pdf

²¹ Congressional Budget Office Letter to Honorable Nancy Pelosi, Speaker of the House, on the Conference Agreement for the American Recovery and Reinvestment Act, February 13, 2009.

<http://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/99xx/doc9989/hr1conference.pdf>

I. Lack of Clear Path Toward Interoperability

Supporters of the HITECH Act have argued that it was enacted to facilitate the electronic sharing of data among health care providers. This function, called “interoperability,” was envisioned to encourage physicians, hospitals, and other health care providers across the country to share patient information, such as medical histories or results of diagnostic tests, through a secure network. Supporters view this network as necessary to achieve the potential cost savings and quality improvements promised by health IT. Sharing patient information was supposed to improve care and allow physicians to coordinate by preventing duplicate testing and preventing harmful drug interactions.



Interoperability is the key to achieving efficiencies in care with health IT; however, interoperability has to date proven very difficult to establish. Ideally, hundreds of thousands of providers, from small family practitioners to very large hospital systems, all need to be using a network and infrastructure that allows for the sharing of information. The network will have to be robust and secure enough to prevent any misuse of sensitive patient information. And such a system has to somehow be developed to work with the hundreds of thousands of IT systems already in place. Moreover, this system must also be flexible enough to accommodate future changes in technology. Additionally, this system must be affordable and simple enough for the wide range of providers to implement.

We are seriously concerned that, despite the billions of taxpayer dollars spent and providers who may be penalized, CMS does not yet seem to have an adequate plan to achieve secure, meaningful interoperability. A lack of meaningful interoperability means \$35 billion and years of effort are at risk of being wasted.

RESPONSE:

The approach to tackling interoperability is clearly delineated in the statement above. The system must be simple to use, flexible to adjust to future technological developments, lightweight, intuitive, and actually complete the loop that makes the effective transition from paper to digital health records. This type of technology does currently exist and can be implemented quickly, even for the most technically challenged participants within the healthcare community.

Interoperability is not difficult to achieve. However, there is currently little incentive for the EHR vendors to cooperate in regard to exchanging patient specific data. There is still a very aggressive “land grab” going on that can negatively affect the healthcare communication landscape. With the re-certification process facing the EHR vendor community, many of the small to mid-sized vendors will be squeezed out of the market, placing greater control in the hands of the largest vendors, who are not always the best vendor of choice. Contributing factors will be the inclusion of an interoperable network and patient portal, a prime requirement for Meaningful Use Stage 2 recertification, the actual cost of recertification, and the unwillingness of the major vendors to cooperate and actually make interoperability work.

The fear is major vendors have planted the seeds in Washington that the technology does not yet exist, it is too complex, or it can never address all of the healthcare issues surrounding secure communications within the healthcare community. This is simply not true. The technology does exist and can be used right now with no other agenda except providing a secure communication network capable of transporting clinical, discrete patient specific data without requiring permission, integration, or cooperation of the major EHR vendors.

Three Stages of HITECH Implementation

As stated in the HITECH Act, one of the purposes of the Office of National Coordinator for Health IT is to “improve the coordination of care and information among hospitals, laboratories, physician offices, and other entities through an effective infrastructure for the secure and authorized exchange of health care information.”²² Coordination is primarily achieved through interoperability, and in an effort to achieve

²² Section 3001 of the American Recovery and Reinvestment Act of 2009. Public Law 111-5.
<http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf>

interoperability, the Office of National Coordinator for Health IT and CMS adopted regulations that create a staged approach where eligible providers will proceed through three stages of requirements. Before focusing on interoperability, these stages largely focus on achieving “meaningful use,” or the ability to use software to achieve government-established milestones largely within a single provider or practice.

Stage 1 requires eligible providers and hospitals to select from both a core set and a menu set of objectives. To achieve Stage 1 meaningful use, the provider or hospital must satisfy all of the core set and a percentage of the menu set objectives.²³ For Stage 2, eligible providers and hospitals must meet Stage 1 requirements for a 90-day period in the first year of participation in the meaningful use program and for a full year in the second year of participation.²⁴ Stage 2 also involves a growing and more complex set of core and menu objectives over those required in Stage 1. None of the required core or menu objectives in Stage 2 requires communication with other health care providers. This means steps towards interoperability are neither being required nor measured. Examples of some of the 17 required core objectives for Stage 2 include:

- recording demographic information,
- incorporating clinical lab-test results into Certified EHR technology, and
- recording smoking status for patients 13 years old or older.

While the Stage 2 requirement to “submit electronic data to immunizations registries” is a small step towards the sharing of health information, it does not require providers to effectively and securely share this data with other providers. Although a request for comments was published in the Federal Register for Stage 3, Stage 3 regulations have not been promulgated, and CMS recently announced a delay in rulemaking for Stage 3.²⁵ We applaud CMS for listening to stakeholder concerns about the speed of implementation of the program.

Misplaced Focus on Use of Technology Within Silos Rather Than Interoperability

Unfortunately, the program as laid out by CMS and the Office of National Coordinator for Health IT continues to focus less on the ability of disparate software systems to talk to one another and more on providing payments to facilities to purchase new technologies. We have seen this focus demonstrated in the following ways:

- The sequencing of regulations from the Office of National Coordinator for Health IT and CMS does not give providers a realistic timeframe during which to achieve meaningful use, despite the fact that the Office of National Coordinator for Health IT and CMS say that the meaningful use program is an important step on the path to interoperability.

²³ “Stage One of Meaningful Use.” Centers for Medicare and Medicaid Services. Last modified September 20, 2012. http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html

²⁴ “Stage Two of Meaningful Use.” Centers for Medicare and Medicaid Services. Last modified November 28, 2012. http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Stage_2.html

²⁵ Vaidya, Anuja. “CMS to Delay Stage 3 Meaningful Use Requirements.” *Becker’s Hospital Review*, March 7, 2013. <http://www.beckershospitalreview.com/healthcare-information-technology/cms-to-delay-stage-3-meaningful-use-requirements.html>

- CMS' failure to systematically and clearly address meaningful groundwork for interoperability at the start of the program could lead to costly obstacles that are potentially fatal to the success of the program.

The current approach to implementing the HITECH Act places a priority on pushing money out the door to get technology into doctors' offices and hospitals, but fails to ensure that technology will be used for its intended purpose. David J. Brailer, the former health information czar under President George W. Bush, warns the approach used to advance the use of EHRs has suffered from a "colossal strategic error" by creating a "race to adopt" mentality that lacks the forethought of pushing toward real interoperability.²⁶

RESPONSE:

We agree with the statement above. The regulations never took into account one basic principle: the need for effective transitions. How is a record actually moved from point A to point B while still protecting patient privacy issues? Right now there is a major "land grab" going on that is being won by all the big vendors and hospital systems. These vendors currently have no incentive to cooperate or help competitors in this field. Moreover, some vendors have even refused to allow the sharing of medical records or created fictional barriers designed to discourage cooperation. Some vendors, as recently presented at the national Health Information and Management Systems Society (HIMSS) conference in Atlanta this past March, have announced a cooperative health information exchange, but no progress has been made on such an exchange.

Rushing Through Stages of Implementation Does Not Allow Adequate Time to Ensure Meaningful Use, a Necessary Step to Interoperability

CMS currently has an aggressive, one-size-fits-all implementation schedule to achieve meaningful use, which does not account for the different abilities of providers to comply with the requirements. For example, some technologically integrated suburban hospitals are being held back from using more advanced capabilities, while small, rural physicians' offices are being overwhelmed by one-size-fits-all requirements.



Stage 1 requirements are effectively applied uniformly and on the same timeline to all providers across the country. This one-size-fits-all requirement ignores the fact that different providers and hospitals had vastly different capabilities at the onset of Stage 1 and overlooks the unique differences between rural solo practitioners, hospitals, older providers, specialty practices, and smaller practices.^{27,28} CMS envisions Stage 1 as the initial gateway on the path to meaningful use. However, if the Stage 1 requirements hinder the ability of providers to take the first step due to unachievable aims, meaningful use becomes that much more difficult to achieve.

²⁶ Abelson, Reed and Julie Creswell. "In Second Look, Few Savings From Digital Health Records." *New York Times* January 11, 2013. http://www.nytimes.com/2013/01/11/business/electronic-records-systems-have-not-reduced-health-costs-report-says.html?_r=0

²⁷ Moukheiber, Zina. "Government Should Slow Down Race to Implement Electronic Health Records." *Forbes* January 17, 2013. <http://www.forbes.com/sites/zinamoukheiber/2013/01/17/government-should-slow-down-race-to-implement-electronic-health-records/>

²⁸ Letter from American Medical Association to Office of the National Coordinator for Health Information Technology, January 14, 2013. <http://www.ama-assn.org/resources/doc/washington/stage-3-meaningful-use-electronic-health-records-comment-letter-14jan2013.pdf>

In the final rule for Stage 1, CMS stated it “expect[s] to update the meaningful use criteria on a biennial basis, with Stage 2 criteria by the end of 2011 and the Stage 3 criteria by the end of 2013.”²⁹ While CMS modified this timeline by delaying Stage 2 by one year and recently announced a delay of Stage 3 rulemaking, the aggressive deadlines may not allow enough time to ensure that all providers are truly gaining *meaningful* use of their EHRs. If providers are not able to achieve meaningful use of their new technologies, they will not be in a position to share electronic records with other providers at the interoperability stage. This dynamic threatens to waste the funds spent on the technology as well as undermine the potential of the cost-savings and improved quality care that come from interoperability. Even worse, on top of this, providers will be penalized for not all reaching a common milestone.

RESPONSE:

We also agree with the statement above. There is a vast difference between medical practices, HIEs, hospitals, and other healthcare facilities such as assisted living, nursing homes, emergency care, and independent surgery centers. However, the basic concept and requirement is the same. That is, simply stated: 1) create and capture a patient encounter electronically (office visit, lab test, imaging, hospital visit etc); 2) securely store the record with easy, on-site access; and, 3) transmit that record from where it resides to where it needs to be within a secure environment. Today, there are several hundred certified EHR and HIS systems available in the marketplace. The answer is not to over-regulate or try to enact legislation to resolve this problem of diversity in EHR requirements, but to take the steps that have already found to be very effective. That is, complete the practice assessment and then line up the individual work flow with a properly certified HER. To a significant extent, the medical community, academics, vendors, and the federal government are over-complicating what can be a simple solution.

Stage 2 and 3 Rules Lack the Benefit of Appropriate Data Review

On September 4, 2012, CMS released the final rule for Stage 2 of meaningful use of EHRs following an announced one-year delay in implementation.³⁰ CMS published this regulation without fully understanding both the strengths and weaknesses of the incentive program during Stage 1. Moreover, CMS released interim Stage 3 requirements and sought comments regarding Stage 3 of meaningful use on November 26, 2012, well before the end of Stage 1.³¹ Within a six-month period, CMS implemented Stage 1, published a final rule for Stage 2, and began seeking feedback for Stage 3. At a time when reports continue to be released questioning the effectiveness of EHR adoption, it is imperative that CMS conduct appropriate data review before accelerating into Stage 2 and Stage 3.³² It was prudent of CMS to heed stakeholder input and delay Stage 3 rulemaking because in order for the HITECH Act to be successful, it may be necessary for the administration to recalibrate their goals and reengage stakeholders to ensure their concerns are addressed and stakeholder insights are applied.



²⁹ Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule. 75 Fed. Reg. 44314, July 28, 2010. <http://www.gpo.gov/fdsys/pkg/FR-2010-07-28/pdf/2010-17207.pdf>

³⁰ Medicare and Medicaid Programs; Electronic Health Record Incentive Program-Stage 2; Final Rule. 77 Fed. Reg. 53968, September 4, 2012. <http://www.gpo.gov/fdsys/pkg/FR-2012-09-04/pdf/2012-21050.pdf>

³¹ Office of the National Coordinator for Health Information Technology; Health Information Technology; HIT Policy Committee: Request for Comment Regarding the Stage 3 Definition of Meaningful Use of Electronic Health Records, 77 Fed. Reg. 7044, November 26, 2012. <http://www.gpo.gov/fdsys/pkg/FR-2012-11-26/pdf/2012-28584.pdf>

³² Ryan, Andrew M., et al. "Small Physician Practices In New York Needed Sustained Help To Realize Gains In Quality From Use Of Electronic Health Records." *Health Affairs* 32.1 (2013): 53-62.

A number of stakeholders have expressed concerns about the speed of implementation. According to a letter to CMS from the American Hospital Association, evidence indicates “the digital divide is widening, with large and urban hospitals reaching much higher rates of adoption than smaller and rural facilities.”³³ Placing an advanced hospital system in the same pipeline as a rural solo practitioner has created problems in providing realistic timelines for all hospitals and providers. Stage 3 proposed rules should address how gaps in provider abilities to achieve interoperability will be addressed.

Lack of Initial Focus on Interoperability Has Created Obstacles to the Success of the Program

Achieving meaningful use occurs when a provider meets established federal requirements within the silo of that physician’s office or hospital. While mastering the use of information within a hospital or physician’s office is critical, more attention needs to be paid to ensuring a path to interoperability has been clearly established.



To date, the lack of unified, well-specified standards is a chief impediment to achieving interoperability. According to a survey and report published by the *Bipartisan Policy Center* and *Doctors Helping Doctors Transform Health Care*, more than 70 percent of clinicians said that a lack of interoperability was what kept them from electronically sharing information.³⁴ We recognize that the Health IT Standards Committee is actively pursuing the goal of unified standards, but we believe more emphasis should be placed on unified standards as a part of the EHR certification process. We are concerned that a lack of established interoperability standards from the beginning has resulted in vendors using vastly different terms, methods, and approaches to designing their health IT systems. This significant variation increases the likelihood that these systems will be unable to talk to and understand one another.

Given the requirements of Stage 2, the leap required from Stage 2 requirements to interoperability between unaffiliated health care systems that operate different software systems is unlikely to be accomplished by Stage 3. This dynamic raises serious concerns about the future of the program and requires the Office of the National Coordinator for Health IT and CMS to develop a workable plan to achieve interoperability.

RESPONSE:

Trying to regulate integrated interoperability at the EHR vendor level by creating various standards does not advance the goals of the meaningful use program. In fact, certain standards already exist. CCDs / CCRs are the only standard required right now in order to move medical records between systems (if a secure network is in place for transportation and communication). For example, take the current phone system in this country and throughout the world. Initially, everything was hard wired by one company and the devices to plug into the system were manufactured by the same company. After de-regulation, everything changed. Today, we have a hard wired communication network as the base service, but it can be accessed through cell phones, wireless devices, cable, satellite, and more. The interoperable

healthcare system needs to be looked at exactly the same way. The individual EHRs represent the access into a common secure communication and transport network. If all users adopt CCR or CCD formatting, which is now required, then a common network will foster interoperability.

³³ American Hospital Association. "Letter to Acting Administrator Marilyn Tavenner on Stage 2 Notice of Proposed Rule Making," April 30, 2012. <http://www.aha.org/advocacy-issues/letter/2012/120430-cl-cms0044p.pdf>

³⁴ *Accelerating Electronic Information Sharing to Improve Quality and Reduce Costs in Health Care*. Bipartisan Policy Center Health Information Technology Initiative, October 2012. [http://bipartisanpolicy.org/sites/default/files/BPC%20Accelerating%20Health%20Information%20Exchange format.pdf](http://bipartisanpolicy.org/sites/default/files/BPC%20Accelerating%20Health%20Information%20Exchange%20format.pdf)

II. Misuse of EHRs May Actually Increase Health Care Costs

Recent evidence indicates that, contrary to initial projections, health IT as currently being used may unfortunately increase health care spending. For years, the arguments for adopting EHRs have focused on the promise of reduced costs to taxpayers and patients, as well as increased efficiency and quality in health care.³⁵ However, recent evidence indicates the push towards EHRs could instead increase utilization of unnecessary, more costly procedures, and, consequently, increase overall health care spending, which results in higher costs for patients and taxpayers. This means that the current health IT policy may be headed in exactly the wrong direction. We want to ensure the path of the program will produce a positive long-term return on investment of taxpayer dollars in EHRs.

Electronic Health Recodes May Facilitate “Code Creep”

Medical codes are used by providers and hospitals to communicate to a payer, such as Medicare or private health insurance, the nature of the care that was provided to the patient. The codes are assigned a dollar value, and higher acuity care for sicker patients is reimbursed at a higher rate. According to a number of articles recently reported in academic journals and the media, the use of EHRs may be driving up costs via a phenomenon referred to as “code creep.”^{36,37}

For example, one form of code creep was highlighted by the *New York Times*: “Some [electronic health record systems] can automatically generate detailed patient histories, or allow doctors to cut and paste the same examination findings for multiple patients – a practice called cloning – with the click of a button or the swipe of a finger on an iPad, making it appear that the physician conducted more thorough exams than, perhaps, they did.”³⁸

Despite conventional wisdom that the wide adoption of health IT would decrease unnecessary tests and imaging as physicians had better electronic access to records, other early evidence actually suggests the opposite. Health IT may have increased the likelihood that duplicative, unnecessary care, such as redundant testing or procedures, will be done. According to a study published in the *Journal of the American Medical Association*, data



PATIENT:		01608034780
CLAIM NUMBER:		
DATE CLAIM RECEIVED:		06/09/10
DATES OF SERVICE	PROCEDURE CODE	
05/21/10-05/21/10	82272	PU
05/21/10-05/21/10	94010	PULMO
05/21/10-05/21/10	94375	CARDIOVASCULAR SERV
05/21/10-05/21/10	93000	VENIPUNCTURE
05/21/10-05/21/10	36410	
		Total:

³⁵ *Health Information Technology: Can HIT Lower Costs and Improve Quality?* RAND Health, 2005.

http://www.rand.org/content/dam/rand/pubs/research_briefs/2005/RAND_RB9136.pdf/

³⁶ Schulte, Fred, et al. “How doctors and hospitals have collected billions in questionable Medicare fees,” *Washington Post* September 15, 2012. http://articles.washingtonpost.com/2012-09-15/national/35496252_1_data-codes-medicare

³⁷ Abelson, Reed, and Julie Creswell. “In Second Look, Few Savings From Digital Health Records.” *New York Times* January 11, 2013. http://www.nytimes.com/2013/01/11/business/electronic-records-systems-have-not-reduced-health-costs-report-says.html?_r=0

³⁸ Abelson, Reed, and Julie Creswell. “In Second Look, Few Savings From Digital Health Records.” *New York Times* January 11, 2013. http://www.nytimes.com/2013/01/11/business/electronic-records-systems-have-not-reduced-health-costs-report-says.html?_r=2&

indicates an increase in use of clinical services when providers use electronic health records.³⁹ In fact, some have attributed a portion of Medicare's increased billings over the last five years to the significant increase in EHR systems.⁴⁰

Code creep can occur in nearly any health care setting that is reimbursed according to medical codes, and it may be unintentional. Some medical providers emphasize that the use of EHRs simply makes it easier to do the necessary documentation that satisfies the requirements for higher reimbursement codes.

While there is currently a lack of conclusive data that can authoritatively answer all relevant questions about the code creep phenomenon, it is clear CMS is not doing enough to address the issue. In the fall of 2012, when congressional staff questioned a CMS official about the possibility of code creep, the high-ranking CMS official effectively said CMS could not confirm that code creep is occurring for at least two years because of the lag in collecting and analyzing data and that consequently no agency actions were needed at the time to prevent unnecessary billing. When staff pressed the official on the wisdom of waiting two years—half of a presidential term—to determine if there is indeed code creep, the official merely demurred about the need for better data and the possibility of future adjustments in Medicare payments. While we appreciate caution, with the Medicare program facing insolvency it is unacceptable for CMS to wait for two years on this potential threat to Medicare. Sooner rather than later, CMS needs to evaluate the Medicare claims data for code creep.

“Cloned” or Copied Records Can Increase Medical Errors

Unfortunately, health IT adoption may have a negative impact on patients that is actually far graver than unintended financial impacts. There is a growing body of evidence that indicates some providers may simply copy and paste information in medical records, which represents a significant increase in the risk of medical errors by potentially including inaccurate, old, or out-of-date patient information in a patient record that can jeopardize patient safety and increase costs.⁴¹ Similarly, others have raised the issue that some health IT applications actually perpetuate cloning records – copying key data from one EHR to another. While it is not inherently wrong for a provider to be able to incorporate standard protocols or care practices into an EHR, any kind of automated cut-and-paste process increases the likelihood of errors or omissions – errors which could even be life-threatening.



³⁹ Palen, Ted E., et al. "Association of Online Patient Access to Clinicians and Medical Records With Use of Clinical Services." *Journal of the American Medical Association* 308.19 (2012).

<http://jama.jamanetwork.com/article.aspx?articleid=1392562>

⁴⁰ Abelson, Reed, et al. "Medicare Bills Rise as Records Turn Electronic." *New York Times* September 21, 2012.

<http://www.nytimes.com/2012/09/22/business/medicare-billing-rises-at-hospitals-with-electronic-records.html>

⁴¹ Stokes, Trevor. "Copying Common in Electronic Medical Records." *Reuters* January 7, 2013.

<http://www.reuters.com/article/2013/01/04/us-electronic-medical-records-idUSBRE9030IJ20130104>

The ability to quickly and easily generate documentation data deserves careful scrutiny as both a benefit and a risk of increased use of health IT. Without proper oversight it is especially concerning, particularly in light of the way the Medicare system currently uses claims data instead of patient outcome-based information to reimburse providers and monitor global changes in clinical patterns and practices. More needs to be done to ensure that the software programs that are sold by government-endorsed vendors and paid for by taxpayer dollars are held to the highest standards and promote the ultimate end goal of safely and effectively sharing health information.

While some analysis suggesting increased health care costs due to EHRs pre-dates the implementation of Stage 1 of the program, we believe this only further underscores the need for more rigorous data analysis of Stage 1 before moving forward into Stages 2 and 3.

III. Insufficient Oversight Has Put Taxpayer Money at Risk

Inspector General Recommends Additional Oversight of Self-Attestation

One of the key program vulnerabilities of the current HITECH program is that providers simply self-report to CMS that they have met meaningful use criteria in order to receive federal funds. This is a startling lack of program integrity. In few other government programs can an applicant simply claim eligibility without offering some documentation. This would be like an individual claiming to have won the lottery but not being required to produce the winning lottery ticket in order to collect the payout.



A recent report by the Department of Health and Human Services Office of the Inspector General (OIG) confirms this is a key program vulnerability, and the report heavily criticizes CMS's inability to effectively monitor eligible providers as they self-attest to meet the meaningful use requirements.⁴² The OIG reviewed documents submitted to CMS from providers and hospitals and analyzed the data to ensure it met program requirements. In its report, the OIG warned that, due to several program factors, it is very possible CMS may have paid providers who are not actually achieving meaningful use requirements.⁴³ In fact, the report's authors are aware of a handful of cases anecdotally where providers self-attested for meaningful use payments but were not eligible, based on the program's criteria. These cases have been referred for further investigation.

At a time when the EHR incentive program is providing billions of taxpayer dollars in payments to providers and hospitals, it is unconscionable that CMS has not yet taken sufficient steps to ensure only eligible providers receive payments. It is essential that proper oversight is in place not only to ensure meaningful use of EHRs through the three stages, but also to prevent those providers or hospitals that are not meeting the required standards from receiving incentive payments from CMS.

⁴² Department of Health and Human Services Office of Inspector General. *Early Assessment Finds That CMS Faces Obstacles in Overseeing the Medicare EHR Incentive Program*. November 28, 2012. <https://oig.hhs.gov/oei/reports/oei-05-11-00250.pdf>

⁴³ Department of Health and Human Services Office of Inspector General. *Early Assessment Finds That CMS Faces Obstacles in Overseeing the Medicare EHR Incentive Program*. November 28, 2012. <https://oig.hhs.gov/oei/reports/oei-05-11-00250.pdf>

Taxpayer “Dollars Spent” Is an Insufficient Metric of Success

One of the most alarming findings in the OIG report is CMS’ response that, despite the OIG’s warning, it does not agree that more pre-payment review of eligibility is necessary since it could delay incentive payments.⁴⁴ Oversight into fraud and abuse vulnerabilities in EHRs continues to be a priority for the OIG, as indicated in its Fiscal Year 2013 work plan.⁴⁵

CMS and the Office of the National Coordinator for Health IT said they disagreed with the OIG recommendation due to concerns about delays in incentive payments to providers and hospitals, and a closer review of the data confirms that CMS may be overly focused on getting payments out the door. In fact, it appears the metric used to measure the success of the EHR program is simply a “cash out the door” measure: federal taxpayer dollars paid to providers.

But as OIG noted, the entire purpose of reviewing applications before payments are made is to prevent the waste of taxpayer dollars on payments to ineligible providers. Thankfully, even though other Health and Human Services agencies are ignoring the issue, oversight into fraud and abuse vulnerabilities in EHRs will continue to be a priority for the OIG this fiscal year.

There are other indications a “cash out the door” metric may be an overly important metric for senior officials at CMS. In the opening session of the 2012 Office of the National Coordinator for Health IT Annual Meeting, Farzad Moshashari, National Coordinator for Health IT, highlighted how much money has been spent and suggested it was the measure of success of the EHR program. He recognized the CMS staff who have helped facilitate the “\$9 billion” that has been provided to states that “had the highest proportion of eligible [providers] paid.”⁴⁶

Additionally, during the meetings of the Health IT Policy Committee, the program metrics discussed are the number of providers participating in the meaningful use program and how much has been paid out in incentive payments.⁴⁷ Those metrics fail to capture the true goal -- provider progress toward interoperability.



⁴⁴ Department of Health and Human Services Office of Inspector General. *Early Assessment Finds That CMS Faces Obstacles in Overseeing the Medicare EHR Incentive Program*. November 28, 2012. <https://oig.hhs.gov/oei/reports/oei-05-11-00250.pdf>

⁴⁵ U.S. Department of Health and Human Services Office of Inspector General. *Work Plan for Fiscal Year 2013*. <https://oig.hhs.gov/reports-and-publications/archives/workplan/2013/Work-Plan-2013.pdf>

⁴⁶ 2012 Office of National Coordinator of Health IT Annual Meeting, “The Year of Meaningful Use: Leaders of the ONC State MU Acceleration Challenge.” December 12, 2012. <http://www.healthit.gov/oncmeeting/webcast/>

⁴⁷ November and December 2012 Health IT Policy Committee, Update from CMS on Medicare and Medicaid EHR Incentive Program PowerPoint, November 7 and December 5, 2012.

http://www.healthit.gov/sites/default/files/hitpc_11_07_12mediincentive_0.pdf;
http://www.healthit.gov/sites/default/files/12_5_12_hitpc_medicare_medicaid_incentives.pdf

Too often in Washington, D.C., politicians and bureaucrats pretend that spending more is doing more. But topline spending is not the most effective measure of the program's success. Giving more providers more money incentivizes the purchase of government-approved health IT systems, but it does not guarantee true interoperability. Reimbursing providers to create technological silos where data is stovepiped is contrary to the goal of creating a system where information about patients can be shared seamlessly between unaffiliated providers.

Insufficient Oversight of Government-Funded Contractors Poses Obstacles to Interoperability

There have been concerning anecdotal reports about a few EHR vendors who use EHR contracts to effectively block or require increased resources for the exchange of data from competitors. The practice essentially only allows the sharing of data between EHRs that originated from the same vendor, effectively locking out data-sharing from other vendors. This dynamic creates patient-safety concerns and can be a barrier to interoperability when data is restricted to one set of providers.

Unless CMS takes strong steps to detect, monitor, and prevent such practices for certified vendors, taxpayers may be subsidizing the purchase of systems that undermine the program's goals by purposely blocking information-sharing with other software from other vendors.

Additionally, physician stakeholders have raised concerns that some of the 2,000 currently certified EHR vendors may not re-certify and will thus no longer offer EHR services. In that event, providers may face difficulties transferring patient data to a new EHR system.⁴⁸ Mitigating steps should be taken by CMS and the Office of the National Coordinator for Health IT to ensure interoperability and data sharing.

We are interested in hearing more about this problem from both stakeholders and the administration and how to address it to achieve interoperability.

RESPONSE:

This section brings up some interesting and very valid concerns. The major vendors perceive the interoperability requirements for re-certification as an overwhelming barrier for the smaller EHR vendors. They are currently positioning themselves as proving they are interoperable within their own system, but that does not address the real issue which is true interoperability across any EHR service. Further, they are unfortunately using scare tactics on providers who do not know better. The patient records belong to the provider and the patient, not the vendor. As an example, if a letter is written using Microsoft Word, Bill Gates does not own that letter nor is his permission needed to send the letter over the Internet or through snail mail. The same holds true with EHR vendors. They own their technology, but not the content created by that technology.

⁴⁸ Letter from American Medical Association to Office of the National Coordinator for Health Information Technology, January 14, 2013. <http://www.ama-assn.org/resources/doc/washington/stage-3-meaningful-use-electronic-health-records-comment-letter-14jan2013.pdf>

EHR vendors can restrict, technically, any attempt at integration into their software to create interoperable links to patient discrete data. In the marketplace, there is more of a willingness to cooperate with an agnostic communications network than with competitors. Congress must begin to question these vendors' practices of restricting the use of medical records – at least to the detriment of the patient – for nothing more than business competition, turf protection, or contributing to the demise of the smaller vendors who, traditionally, provide better service and product.

IV. Long-Term Questions on Data Security and Patient Safety Remain

In 2011, ONC asked the Institute of Medicine (IOM) to evaluate patient safety and privacy concerns regarding electronic health records and identify steps that can be taken to address these concerns.⁴⁹ As stated in the IOM's report, academic and research literature about health IT and patient safety is inconclusive thus far.⁵⁰ This is likely due to a lack of comprehensive and comparable data for EHRs.

Being proactive in anticipating and planning for patient safety concerns is a critical part of the long-term success of EHRs. Providers unsure about protecting the security of patient data will be more likely to opt

out of EHR programs. Additionally, patients will be less likely to engage with their EHR if they feel their information is not secure or care is negatively affected. If unaddressed, these issues could seriously undermine the program.



We recognize that CMS and the Office of the National Coordinator of Health IT face a difficult challenge in ensuring federally incentivized EHRs are sufficiently secure and patient information is protected. However, federal agencies and health care providers are not immune to data security breaches. In 2011, for example, information about 20,000 emergency room patients from a California hospital was posted on a commercial website for nearly a year.⁵¹

Additionally, an OIG report published recently revealed neither entity was doing enough to implement necessary security measures to protect sensitive patient information within their own offices.⁵² If data security and patient privacy have proved to be a challenge within the Office of the National Coordinator for Health IT and CMS within the last two years, it is reasonable to assume that providers and stakeholders may face similar challenges.⁵³

⁴⁹ Institute of Medicine. *Health IT and Patient Safety: Building Safer Systems for Better Care*. November 2011. http://www.iom.edu/~media/Files/Report%20Files/2011/Health-IT/HealthITandPatientSafetyreportbrieffinal_new.pdf

⁵⁰ Institute of Medicine. *Health IT and Patient Safety: Building Safer Systems for Better Care*. November 2011. http://www.iom.edu/~media/Files/Report%20Files/2011/Health-IT/HealthITandPatientSafetyreportbrieffinal_new.pdf

⁵¹ Sack, Kevin. "Patient Data Posted Online in Major Breach of Privacy." *New York Times* September 8, 2011. <http://www.nytimes.com/2011/09/09/us/09breach.html?pagewanted=all&r=0>

⁵² Department of Health and Human Services Office of Inspector General. *Early Assessment Finds That CMS Faces Obstacles in Overseeing the Medicare EHR Incentive Program*. November 28, 2012. <https://oig.hhs.gov/oei/reports/oei-05-11-00250.pdf>

⁵³ Lewis, Nichole. "Federal Agencies Fail Health IT Security Audits." *Information Week*. May 18, 2012. <http://www.informationweek.com/healthcare/security-privacy/federal-agencies-fail-health-it-security/229502471>

Problems with data entry, computer programming errors, and other unforeseen complications can affect the security of patient data and have the potential to jeopardize patient safety. Improper access to EHRs by unauthorized agents also poses a threat to the security of patient information. The OIG shares our concerns with ensuring adequate information technology control standards to protect patient information and plans to continue to monitor this risk.⁵⁴

Patient Safety Concerns Must Be Balanced With Burdens on Providers

No system is completely invulnerable to criminals or reckless actors who do not follow protocols. As systems become more secure, they may be less useful to providers and patients. Therefore, concerns about the security of patient information need to be balanced against the burdens placed on entities that are responsible for the safekeeping and disclosure of the data. It is unclear if HHS has properly considered the safety and security issues, much less the burden, to date.



⁵⁴ U.S. Department of Health and Human Services Office of Inspector General. *Work Plan for Fiscal Year 2013*. <https://oig.hhs.gov/reports-and-publications/archives/workplan/2013/Work-Plan-2013.pdf>

V. Questions Remain About Long-Term Sustainability of the EHR Program

In addition to our concerns about interoperability, costs, oversight, and security, we have an even more basic concern that the \$35 billion effort will be wasted if providers are not able to comply with requirements or maintain the health IT system over the long-term. HITECH was included in a controversial, rushed legislative environment and enacted in the midst of an already complicated and increasingly burdensome regulatory landscape. Multiple overlapping reporting and regulatory burdens will make it difficult for providers to stay abreast of developments and direct the majority of their time to patient care.

The pressure on providers will only further increase when incentive payments turn into penalties. At that point, it will be even more challenging for many providers to maintain health IT systems, which will need to be constantly monitored, managed, and upgraded to keep up with changing technologies.



These long-term risks are even more pronounced for solo practitioners and other small- to medium-size offices that do not have the benefit of achieving economies of scale and spreading their acquisition and maintenance costs over a larger pool of patients. For example, one study of ongoing EHR costs for small and solo practices estimated that the ongoing costs to maintain an EHR system averaged over \$8,000 per provider per year.⁵⁵ Providers are already facing large payment changes and administrative costs due to changes in federal policy and regulations.

Incentives for Compliance to Be Replaced by Penalties for Noncompliance

As the EHR incentive program continues to progress, long-term uncertainty for physicians is still a problem that needs to be addressed as physicians fear the looming penalties. In 2015, physicians and hospitals will begin incurring penalties in the form of decreased Medicare reimbursement for not meeting meaningful use requirements. While it is true EHR adoption has been increasing nationwide, research suggests that most physicians who have already applied for incentive payments or intend to apply for them are not gaining meaningful use under CMS's regulatory standards.⁵⁶ This means that initial estimates overestimated providers in compliance, leaving many more providers out of compliance than originally thought.

To avoid a penalty, those who participated in the EHR incentive program in 2011 and 2012 must demonstrate meaningful use for a full year in 2013, the final year of Stage 1 of meaningful use, to avoid

⁵⁵ Menacehmi, Nir, and Taleah H Collum. "Benefits and drawbacks of electronic health record systems." *Risk Management and Health Care Policy* (May 2011): 47-55. <http://www.dovepress.com/benefits-and-drawbacks-of-electronic-health-record-systems-peer-reviewed-article-RMHP>

⁵⁶ Hsiao, Chun-Ju, and Esther Hing. "Use and Characteristics of Electronic Health Record Systems Among Office-based Physician Practices: United States, 2001-2012." Centers for Disease Control and Prevention. December 6, 2012. <http://www.cdc.gov/nchs/data/databriefs/db111.pdf>

the penalty beginning January 2015.⁵⁷ Furthermore, these providers must then continue to show meaningful use of EHRs every subsequent year in order to avoid future penalties.

According to the Government Accountability Office, participation for 2011, the most recent year data is available from an entity outside of the U.S. Department of Health and Human Services, shows that participation in the program is low. As noted in the table below, less than 40 percent of hospitals are participating in the Medicaid program and less than 20 percent participate in the Medicare program. Even with an increase in participation before 2015, one could project a scenario where more than a third of all hospitals are penalized.

	Medicaid	Medicare
Number (percentage of eligible)	1,964 (39)	761 (16)
Median payment	\$613,512	\$1.7 million
Total payments	\$1.7 billion	\$1.3 billion

Source: GAO⁵⁸

Reports continue to be published regarding the difficulties that established eligible providers and those in smaller practices are having in achieving meaningful use of EHRs. Accordingly, we are concerned about CMS's rigid timeline and insufficient flexibility for providers who face these specific circumstances.^{59,60} In its final rule for Stage 2 of meaningful use, CMS acknowledged various reports regarding these difficulties, but did not seek to provide relief from these burdens.⁶¹

Long-Term Sustainability of EHR Systems Is Questionable Due to Other Financial Pressures on Providers

At a time when the CMS Actuary has projected that future reductions in Medicare reimbursements may produce negative Medicare margins for providers, we are concerned that eligible providers will also be unable to sustain their EHR systems.⁶² Continued maintenance and upgrades of EHR hardware and software systems will require massive investments in information technology infrastructure. However, it is unclear if providers will be able to dedicate the necessary resources for these types of investments in the near future. The unstable financial climate for hospitals and other providers undermines the future sustainability of EHR systems. This issue is intricately tied into concerns about the careful balance that must be struck between data security for patient privacy and the burdens imposed on providers.

⁵⁷ Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule. 75 Fed. Reg. 44314, July 28, 2010. <http://www.gpo.gov/fdsys/pkg/FR-2010-07-28/pdf/2010-17207.pdf>

⁵⁸ Number and Characteristics of Providers awarded Medicaid Incentive Payments for 2011. Government Accountability Office, December 13, 2012. <http://www.gao.gov/products/GAO-13-146R>

⁵⁹ Hsiao, Chun-Ju, et al. "Most Physicians Were Eligible For Federal Incentives In 2011, But Few Had EHR Systems That Met Meaningful Use Criteria." *Health Affairs* 31:5 (2012): 1-8.

⁶⁰ Decker, Sandra L., et al. "Physicians In Nonprimary Care And Small Practices And Those Age 55 And Older Lag In Adopting Electronic Health Records Systems." *Health Affairs* 31:5 (2012): 1108-1114.

⁶¹ Medicare and Medicaid Programs; Electronic Health Record Incentive Program-Stage 2; Final Rule. 77 Fed. Reg. 53968, September 4, 2012. <http://www.gpo.gov/fdsys/pkg/FR-2012-09-04/pdf/2012-21050.pdf>

⁶² CMS Actuary's Estimated Financial Effects of the Patient Protection and Affordable Care Act, As Amended. April 22, 2013. <http://www.cms.gov/Research-Statistics-Data-and-Systems/Research/ActuarialStudies/downloads/PPACA-2010-04-22.pdf>

Multiple Health IT Programs Create a Challenging Regulatory Landscape That Affects Providers' Ability to Satisfy Federal Requirements

As previously noted, health IT policy is governed by a complicated patchwork of overlapping federal legislation and standards. Federal laws and standards are implemented through CMS, the Office of the National Coordinator for Health IT, the Agency for Healthcare Research and Quality, the Health Resources and Services Administration, and the National Institute of Standards and Technology, among others. Additional entities working on standards include the Health Information Security and Privacy Collaboration, which is developing a national privacy and security framework, the Health Information Technology Standards Panel, a public-private effort to develop standards for the certification of health IT products, and the National eHealth Collaborative, a public-private advisory body to make recommendations on health IT adoption and usability. The multiplicity of actors and entities has created a confusing, complicated system of requirements that providers must navigate in order to avoid mandated penalties for noncompliance. These compliance burdens are largely not in sync and create a tangle of requirements that may be well-intentioned, but will likely be opaque and confusing to stakeholders. Moreover, these panels

need sufficient time to learn from each stage, develop appropriate recommendations, and give vendors and providers time to update and respond to the new demands. This speaks to the concern that the pace of implementation prior to CMS's announcement of a delay in Stage 3 rulemaking did not allow for this type of thoughtful approach.



Serious Program Vulnerabilities Demand Consideration; CMS Decision to Delay Appropriate

Based on a range of objective data, it is clear that the current payment structure of the EHR incentive program does not provide enough oversight or safeguards to ensure the proper stewardship of taxpayer dollars. Moving rapidly through the three stages without providing clear and proper oversight of the EHR incentive program is a short-sighted approach. It prevents CMS and the Office of the National Coordinator for Health IT from studying findings reported by eligible providers and hospitals to ensure the long-term success of the HITECH Act.

We seek comments on whether it would be in the best interest of CMS, the Office of the National Coordinator of Health IT, vendors, providers, taxpayers, and other stakeholders to hit “pause” while reexamining the current procedures put in place to safeguard and ensure meaningful use of EHRs prior to forging ahead with Stages 2 and 3. We are not alone in our concern on this issue. For example, the American Medical Association and other health care stakeholders have asked CMS and the Office of the

National Coordinator of Health IT to hire an outside entity to evaluate the incentive program's performance before quickly rushing into future stages.^{63,64}

We are pleased CMS has effectively announced such a pause by delaying promulgating Stage 3 regulations and seeking to work with stakeholders. We seek comments on what steps CMS needs to take before implementing Stage 3.

⁶³ Conn, Joseph. "AMA Calls for Outside Evaluation of Electronic Health Records Incentives." *Modern Healthcare* January 14, 2013. <http://www.modernhealthcare.com/article/20130114/NEWS/301149961>

⁶⁴ Conn, Joseph. "HIMMS, ACP also weigh in on Stage 3 MU." *Modern Healthcare* January 16, 2013. <http://www.modernhealthcare.com/article/20130116/NEWS/301169956>

Conclusion

Transformations in health IT will significantly change how health care is provided in this country. Americans want to search for medical information online, check drug interactions or symptoms with their smart phones, and e-mail their doctors. Physicians can now access digital records of a patient even if they are in another city, state, or country. Clinical notes are recorded with increasing speed and ease, and other transformations offer the promise of increased efficiency, reduced costs, and improved quality of care.

However, the details of federal law and regulation may be inadvertently incentivizing unworkable, incoherent policy goals that ultimately make it difficult to achieve interoperability. Congress, the administration, and stakeholders must work together to “reboot” the federal electronic health record incentive program in order to accomplish the goal of creating a system that allows seamless sharing of electronic health records in a manner that appropriately guards taxpayer dollars. Fulfilling the goal of increasing efficiency in the health care system; reducing costs for payers, providers, and patients; and improving quality of care for patients is a challenging task. In order to succeed, the following implementation deficiencies must be addressed:

- **Lack of Clear Path Toward Interoperability**
- **Increased Costs**
- **Lack of Oversight**
- **Patient Privacy at Risk**
- **Program Sustainability**

We present this white paper in an effort to initiate a dialogue with the administration and the stakeholder community. The purpose of this paper is to foster cooperation between all stakeholders – including providers, patients, EHR vendor companies, and the Department of Health and Human Services – to address the issues raised in this white paper, evaluate the return on investment to date, and ensure this program is implemented wisely.